THE HONORABLE JOHN H. CHUN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

AVELARDO RIVERA and YASMINE ROMERO, individually, and on behalf of all others similarly situated, Plaintiffs, v. AMAZON WEB SERVICES, INC., Defendant.	No. 2:22-cv-00269-JHC AMAZON WEB SERVICES, INC.'S RULE 12(b)(6) MOTION TO DISMISS FIRST AMENDED CLASS ACTION COMPLAINT NOTE ON MOTION CALENDAR: November 11, 2022 ORAL ARGUMENT REQUESTED

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF CONTENTS

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

TABLE OF AUTHORITIES

Page(s)

CASES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

STATUTES

OTHER AUTHORITIES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

INTRODUCTION

This case is a brazen attempt to expand the Illinois Biometric Information Privacy Act ("BIPA") far beyond what its authors could have possibly intended. It should be dismissed in its entirety and with prejudice under Federal Rule of Civil Procedure ("Rule") 12(b)(6).

Plaintiffs Avelardo Rivera and Yasmine Romero claim that they took multiple remote tests (i.e., "take home" tests) while they were students at Illinois colleges. To protect the integrity of those tests, Plaintiffs' colleges required Plaintiffs to use an online test proctoring service provided by ProctorU, Inc. ProctorU, in turn, required Plaintiffs to submit images of their faces, and images of valid identification documents, to ProctorU. According to Plaintiffs, ProctorU then uploaded those images to its Amazon Web Services ("AWS") account and used AWS's Rekognition software to compare the images in order to verify Plaintiffs' identities.

Plaintiffs do not allege that they interacted with AWS in any way, or that AWS was even aware of their use of ProctorU's service. Nor do Plaintiffs allege that AWS committed a single act in Illinois. Nevertheless, Plaintiffs seek to hold AWS liable under BIPA, an Illinois law that governs the possession and collection of biometric data. Curiously, Plaintiffs have chosen not to sue their colleges, which "requir[ed]" them to use ProctorU's service, or ProctorU, which "required" them to submit images of themselves and then analyzed those images to confirm their identity—suggesting strongly that this case is motivated by AWS's deep pockets rather than any actual harm to Plaintiffs. Dkt. 44 ("FAC") ¶¶ 35, 39–40, 46–47.

In any case, Plaintiffs' novel attempt to sue AWS, which acted as nothing more than a "behind-the-scenes" cloud-service provider for ProctorU, fails for multiple reasons. *Id.* ¶ 5.

First, Plaintiffs' attempt to sweep back-end cloud-service providers into BIPA's scope is inconsistent with any rational reading of the law. Plaintiffs do not, and cannot, allege that AWS "possessed" or "collected" their data within the meaning of BIPA, and they therefore cannot allege that BIPA applies to AWS at all. Further, interpreting BIPA to apply to AWS in this case would produce absurd and unworkable results that this Court cannot condone.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Second, BIPA does not apply outside Illinois. So, to avoid dismissal, Plaintiffs must allege that AWS's purported violations "occurred primarily and substantially in Illinois." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 187 (2005). But Plaintiffs do not, and cannot, allege that AWS engaged in *any* conduct in Illinois. BIPA therefore does not apply.

Third, BIPA itself provides that the law's requirements may not be applied "in any manner" to "financial institution[s]" subject to the federal Gramm-Leach-Bliley Act, which includes Plaintiffs' colleges. 740 ILCS 14/25(c). Forcing AWS to comply with BIPA's requirements in this context inevitably would force Plaintiffs' colleges to comply with BIPA, too. The plain language of BIPA forbids that result and requires dismissal of Plaintiffs' claims.

Fourth, Plaintiffs cannot be "aggrieved" by AWS's purported failure to publish a biometric data retention policy under Section 15(a) of BIPA—an essential element of their claim. Plaintiffs' Section 15(a) claim must be dismissed for that additional and independent reason.

Fifth, even if Plaintiffs could clear all the hurdles above, their claims would still fail *because AWS complied with BIPA*. Specifically, AWS contractually required its customers (including ProctorU) to provide notice, obtain consent, and otherwise fulfill BIPA's requirements with respect to their end users (including Plaintiffs). AWS therefore did everything in its power to comply with BIPA, and Plaintiffs have not alleged AWS could have done more.

Plaintiffs may or may not have valid BIPA claims against their colleges or against ProctorU, the entities that required them to do the things of which they complain. But Plaintiffs certainly have no claims against AWS, which has no relationship to Plaintiffs and merely acted as a back-end, out-of-state service provider for ProctorU. Plaintiffs' claims should be dismissed.

BACKGROUND

A. The Illinois Biometric Information Privacy Act ("BIPA")

Plaintiffs' claims arise exclusively under BIPA, an Illinois state law. BIPA was enacted in 2008 in reaction to the growing use of biometric technology "in the business and security screening sectors," and to address the concerns of members of the public who were "weary of the

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

use of biometrics when such information is tied to finances and other personal information." 740 ILCS 14/5(a), (d). Recognizing that "[t]he use of biometrics . . . appear[ed] to promise streamlined financial transactions and security screenings," the Illinois General Assembly sought to allay the public's concerns by regulating private companies' use of such data. *Id*.

BIPA specifically regulates "biometric identifiers" and "biometric information." A "biometric identifier" means a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. "Biometric information" means any information "based on" a biometric identifier. *Id*. For brevity, AWS refers to "biometric identifiers" and "biometric information" collectively as "biometric data."[1]

BIPA does not prohibit the collection and use of biometric data. Rather, it imposes obligations on private entities if they engage in certain activities with respect to biometric data. For example, under Section 15(a) of BIPA, companies "in possession" of biometric data must develop and comply with "a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying" biometric data within certain timeframes set out in the law. 740 ILCS 14/15(a). And under Section 15(b), companies that "collect . . . or otherwise obtain" biometric data must provide notice and obtain consent before doing so. 740 ILCS 14/15(b).

BIPA's penalties are harsh. "Any person aggrieved" by a violation of the law may sue for actual damages or, alternatively, liquidated damages of $1,000 per violation (for negligent violations) or $5,000 per violation (for "intentional[] or reckless[]" violations). 740 ILCS at 14/20(1), (2). A prevailing party also may recover attorneys' fees and costs. *See* 740 ILCS 14/20(3). The potential for enormous recoveries has inspired a wave of more than 1,500 putative BIPA class actions in recent years. *See* Declaration of Ryan Spear ("Spear Decl.") ¶ 2; *see also*

[1] By referring to "biometric data" throughout this motion, AWS does not concede that it collected, possessed, stored, or otherwise obtained or used any data regarding Plaintiffs. Further, AWS specifically reserves the right to argue, at the appropriate time, that even if it did collect, possess, store, or otherwise obtain or use any data regarding Plaintiffs, no such data qualifies as "biometric identifiers" or "biometric information" within the meaning of BIPA.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

id., Ex. A (U.S. CHAMBER OF COMMERCE INSTITUTE FOR LEGAL REFORM, ILR BRIEFLY, A BAD MATCH: ILLINOIS AND THE BIOMETRIC INFORMATION PRIVACY ACT 4, 7 (Oct. 2021)) (noting the "exponential growth in BIPA litigation," which has disproportionately targeted "small companies" in Illinois).

B. Amazon Web Services ("AWS"), Rekognition, and ProctorU

AWS is "one of the largest providers of cloud computing services," offering its customers "over 200 cloud-based services from data centers globally." FAC ¶¶ 1–2. As the Ninth Circuit has explained, the term "cloud computing" is "based on the industry usage of a cloud as a metaphor for the ethereal internet. . . . An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google." *United States v. Cotterman*, 709 F.3d 952, 965 n.12 (9th Cir. 2013) (en banc) (internal quotation marks and citation omitted). In practical terms, AWS's cloud services allow AWS customers, like ProctorU, to remotely access, use, and control computer servers maintained by AWS to store and process the customers' own data, however the customers see fit. Plaintiffs correctly allege that "[m]illions of customers—from startups to the largest enterprises—use AWS every day." FAC ¶ 2.

One of the cloud-based services that AWS provides to its customers is a software product called "Rekognition." *Id*. ¶ 3. According to Plaintiffs, Rekognition "uses machine vision and algorithmic classification techniques" to analyze electronic images, including images of faces. *Id*. Plaintiffs allege that AWS customers may upload electronic images to their cloud-storage accounts at AWS (known as "S3 buckets") and then run a Rekognition command called "index-faces" to extract biometric data from those images of faces. *Id*. ¶¶ 25–30. Plaintiffs further allege that AWS customers may then use Rekognition's "face-matching" command to determine whether the same person appears in two or more images, and to generate a "[s]imilarity" score, i.e., "a confidence measurement to indicate how strongly Rekognition believes these faces match." *Id*. ¶ 32.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

AWS makes Rekognition available to its customers subject to the terms and conditions in the AWS Customer Agreement. *See* Spear Decl., Ex. C (AWS Customer Agreement) ¶ 1.1 ("You will comply with the terms of this Agreement and all laws, rules and regulations applicable to your use of [AWS] Service Offerings."). The AWS Service Terms, in turn, requires customers who use Rekognition to "provid[e] legally adequate privacy notices to End Users," such as Plaintiffs, and to "obtain[] any necessary consent from such End Users for the processing of" their data. *See id*., Ex. D (AWS Service Terms) ¶ 50.4 (terms applicable to Rekognition); *id*., Ex. C (AWS Customer Agreement) ¶ 1.1 (incorporating AWS Service Terms). The AWS Customer Agreement also makes clear that data collected by customers belongs to customers, and hence that AWS may not "access or use" customers' content "except as necessary to maintain or provide [AWS] Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." *Id*., Ex. C (AWS Customer Agreement) ¶ 3.2.

ProctorU is one of "[t]housands" of companies that use Rekognition in their own products and services. FAC ¶¶ 4, 34. ProctorU allegedly "develops and licenses online test proctoring software for use by students and educational facilities." *Id*. ¶ 34. When a "student takes a test using ProctorU's proctoring software, ProctorU requires students to show their faces and their photo IDs on camera to help verify their identities." *Id*. ¶ 35. And "when [those students] upload their images to ProctorU," ProctorU allegedly "use[s] Amazon Rekognition" to compare the images and confirm students' identities based on those images. *Id*. ¶¶ 36, 41, 48.

Importantly, Plaintiffs do not allege that AWS plays any role in ProctorU's verification process beyond allowing ProctorU to use Rekognition. Nor do Plaintiffs allege that AWS controls the data in ProctorU's S3 buckets, or that AWS interacts with or could interact with ProctorU's users. Indeed, Plaintiffs do not even allege that AWS *knows* when ProctorU collects and stores students' data, let alone that AWS knows when ProctorU collects and stores data from students *in Illinois*. And, equally important, Plaintiffs do not allege that ProctorU's S3 buckets are located in Illinois, or that AWS engaged in any conduct in Illinois.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

C. Plaintiffs' Claims Against AWS

Plaintiffs' claims are based entirely on their use of ProctorU's service. Plaintiffs allege that they each "took multiple tests" at two Illinois schools (the "Colleges") between 2019 and 2020. *Id*. ¶¶ 38–39, 45–46. Plaintiffs allege that their Colleges "requir[ed]" Plaintiffs to use ProctorU's service. *Id*. ¶¶ 39, 46. Plaintiffs further allege that ProctorU "required" Plaintiffs "to submit [their] image as well as an image of a valid identification document in order to be identified." *Id.* ¶¶ 40, 47; *see also id*. ¶ 35 (ProctorU "requires" students to submit images to ProctorU). According to Plaintiffs, ProctorU then used the Rekognition service to confirm their identities based on the images they submitted to ProctorU. *See id*. ¶¶ 41, 48.

Based on those allegations, Plaintiffs assert two claims against AWS. First, they allege that AWS violated Section 15(a) of BIPA by "possess[ing]" their biometric data—that is, the data ProctorU collected and then uploaded to ProctorU's S3 buckets—without publishing "a publicly-available retention and deletion schedule." *Id.* ¶¶ 44, 51. Second, Plaintiffs allege that AWS violated Section 15(b) of BIPA by "collect[ing]" that same data without providing the notice, and obtaining the consent, that Section 15(b) requires when companies collect biometric data. *See id*. ¶¶ 42–43, 49–50. Plaintiffs assert both claims on behalf of themselves and "[a]ll Illinois residents who had their biometric information or biometric identifiers collected, captured, received, possessed, or otherwise obtained by Amazon's Rekognition service and stored in AWS's servers." *Id.* ¶ 52.

D. Procedural Posture

This case was filed on March 7, 2022. *See* Dkt. 1. At that time, Jacinda Dorian was the sole named plaintiff. After AWS's motion to dismiss Ms. Dorian's claims was fully briefed, AWS learned that Ms. Dorian was not, in fact, a ProctorU user. *See* Dkt. 38. AWS promptly brought that issue to the attention of plaintiffs' counsel, who sought and obtained leave to remove Ms. Dorian as the named plaintiff and replace her with the current named plaintiffs. *See* Dkts. 40, 43. AWS now moves to dismiss the claims of the new plaintiffs.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

ARGUMENT

A. AWS Did Not "Possess" or "Collect" Plaintiffs' Data

As a threshold matter, Plaintiffs' claims fail because they cannot allege essential elements of those claims. Plaintiffs cannot allege that AWS "possessed" their data under Section 15(a) of BIPA because they cannot allege that AWS exercised any control or authority over that data. Similarly, Plaintiffs cannot allege that AWS "collected" their data under Section 15(b) of BIPA because Plaintiffs' own allegations make clear that AWS never took any active steps to acquire or obtain the data; rather, it was ProctorU alone that collected Plaintiffs' data. And as explained below, departing from those common-sense readings of BIPA's language would lead to a series of absurd and unworkable results. Plaintiffs' claims should therefore be dismissed.[2]

1. Plaintiffs allege no facts showing that AWS "possessed" their data.

Section 15(a) applies only to private entities "in possession of" biometric data. 740 ILCS 14/15(a). But Plaintiffs do not, and cannot, allege any facts showing that AWS possessed their data within the meaning of Section 15(a).

BIPA does not define "possession." Courts therefore "assume the legislature intended for it to have its popularly understood meaning." *Rosenbach v. Six Flags Ent. Corp*., 129 N.E.3d 1197, 1205 (Ill. 2019) (citations omitted). The Illinois Supreme Court has explained that "possession, as ordinarily understood, occurs when a person *has or takes control* of the subject property or *holds the property at his or her disposal*." *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (internal quotation marks omitted) (emphasis added); *see also* Ill. Crim. Pattern Jury Instr. 4.16 ("actual possession" is "immediate and exclusive control over a thing" and "constructive

[2] As the Court knows, dismissal under Rule 12(b)(6) "can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988), *as amended* (May 11, 1990). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation marks and citation omitted). Dismissal should be with prejudice where, as here, the flaws in a complaint could not be cured by repleading. *See, e.g.*, *Williams v. Nat'l Football League*, No. C14-1089, 2014 WL 5514378, at *4 (W.D. Wash. Oct. 31, 2014), *aff'd*, 671 F. App'x 424 (9th Cir. 2016).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

possession" is "both the power and the intention to exercise control over a thing"). The Ninth Circuit interprets "possession" similarly. *See, e.g.*, *United States v. Kuchinski*, 469 F.3d 853, 861 (9th Cir. 2006) (possession in "electronic context[s]" requires a showing that the person "exercises dominion and control over" the relevant material); Ninth Cir. Crim. Model Jury Instr. 6.15 ("A person has possession of something if the person knows of its presence and has physical control of it or knows of its presence and has the power and intention to control it.").

Here, Plaintiffs do not allege that AWS controlled the data that ProctorU allegedly uploaded to its S3 buckets. *See Ward*, 830 N.E.2d at 560. In fact, Plaintiffs do not even allege that AWS "kn[ew] of [the] presence" of that data. Ninth Cir. Crim. Model Jury Instr. 6.15. That crucial omission is unsurprising given that AWS has "[m]illions" of customers, FAC ¶ 2, each of which may have up to 1,000 S3 buckets in their accounts, *see* Spear Decl., Ex. B at 1 ("Bucket restrictions and limitations" page from AWS's website).[3]

Plaintiffs' failure to allege that AWS controlled (or even knew about) ProctorU's data is fatal to their Section 15(a) claim. And no amount of repleading could cure that defect because AWS simply does not own or control that data. As the publicly available AWS Customer Agreement makes clear, AWS does "not access or use . . . Content [of AWS customers like ProctorU] except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." Spear Decl., Ex. C (AWS Customer Agreement) ¶ 3.2. The AWS Customer Agreement further provides that AWS customers must "ensure that [their] Content and [their] and End Users' use of [their] Content or the Service Offerings will not violate any of the [AWS] Policies or any applicable law." *Id.* ¶ 4.2. And it states, in no uncertain terms, that AWS customers "are solely responsible for the development, content, operation, maintenance, and use of [their] Content." *Id*. Thus, ProctorU

[3] Plaintiffs' FAC relies extensively on AWS's website. *See, e.g.*, FAC ¶¶ 24–26. The Court may therefore consider other portions of AWS's website, and documents available on AWS's website, under the incorporation-by-reference doctrine. *See, e.g.*, *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005); *Loomis v. Slendertone Distrib., Inc.*, 420 F. Supp. 3d 1046, 1063 (S.D. Cal. 2019).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

"maintain[s] *full control*" of any "content that [it] upload[s] to" AWS's servers, and AWS does "not access or use [the] content for any purpose without [ProctorU's] agreement." Spear Decl., Ex. E at 1–2 (AWS Data Privacy FAQ) (emphasis added).

Plaintiffs' allegations are entirely consistent with those publicly available terms and disclosures. Plaintiffs allege that only ProctorU exercised control over their alleged biometric data, and thus that only ProctorU "possessed" that data within the meaning of BIPA. *See Ward*, 830 N.E.2d at 560. According to Plaintiffs, it was ProctorU that "required [them] to submit [their] image[s] as well as an image of a valid identification document in order to be identified," FAC ¶¶ 40, 47; it was ProctorU that allegedly "perform[ed] facial recognition on" the images Plaintiffs submitted to ProctorU, *id*. ¶¶ 41–48; and it was ProctorU that determined how and where to store and use the data generated by Plaintiffs' use of ProctorU's service, *see id*. ¶¶ 27–36. Nothing in Plaintiffs' FAC suggests that AWS had any knowledge of those events, or that AWS exercised, or could have exercised, any control over the data involved. Thus, it defies common sense to say that AWS "possessed" Plaintiffs' data. Rather, any such data remained subject to ProctorU's exclusive "dominion and control," and therefore wholly within ProctorU's possession, at all times. *Kuchinski*, 469 F.3d at 861.

Courts have dismissed Section 15(a) claims against other companies acting in a service provider capacity, as AWS allegedly did here, on the same grounds. In *Heard v. Becton, Dickinson & Co.*, for example, the Northern District of Illinois dismissed a Section 15(a) claim against a company that provided fingerprint-based access devices for hospitals. *See* 440 F. Supp. 3d 960, 962 (N.D. Ill. 2020). There, as here, the plaintiff alleged that the defendant "stored" alleged biometric data "in [its] systems." *Id*. at 968. But that was not enough to adequately allege *possession*. Mere storage, the *Heard* court explained, did not suggest "any form of control" or imply that the defendant "could freely access the data." *Id.* at 968–69. The same principle applies in this case. Plaintiffs have alleged, at most, ProctorU's use of AWS cloud servers to *store*

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

ProctorU's data in ProctorU's S3 buckets. That is not enough to allege *possession* by AWS under Section 15(a).[4]

Similarly, in *Jacobs v. Hanwha Techwin America, Inc*., a different judge in the Northern District of Illinois dismissed a Section 15(a) claim against a manufacturer and distributor of security cameras that were allegedly used to performed facial recognition on T.J. Maxx shoppers. *See* No. 21 C 866, 2021 WL 3172967, at *3 (N.D. Ill. July 27, 2021). There, as here, the plaintiff failed to allege that the defendant "exercised control over plaintiff's data or otherwise held plaintiff's data at its disposal." *Id.* (citation omitted). As a result, the *Jacobs* court could not "draw the reasonable inference that defendant was 'in possession' of [plaintiff's] biometric data." *Id*. Plaintiffs' Section 15(a) claim in this case suffers from the same flaw, and it should be dismissed for the same reasons.

In addition to misreading the text of Section 15(a), Plaintiffs' attempt to stretch the concept of "possession" to include AWS invites absurd results. *See, e.g.*, *Solon v. Midwest Med. Recs. Ass'n*, 236 Ill. 2d 433, 441 (2010) (when interpreting statutes, courts must "presume that the legislature did not intend absurd, inconvenient, or unjust consequences").

Again, where Section 15(a) applies, it requires a private entity to publish a retention and deletion schedule *and* to "permanently destroy[]" biometric data "when the initial purpose for collecting or obtaining" the data "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). But Plaintiffs do not explain how AWS could comply with those requirements with respect to data uploaded by customers like ProctorU, nor could they. Plaintiffs do not allege that AWS "interact[s] with" its customers' end users at all. Rather, they allege that "Rekognition is a behind-the-scenes service for businesses" like ProctorU. FAC ¶ 5.

[4] The *Heard* court later allowed the plaintiff's Section 15(a) claim to survive a second motion to dismiss. *See Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 840 (N.D. Ill. 2021). But the court did so only after the plaintiff amended the complaint to add plausible allegations that the defendant "exercise[d] some form of control" over the plaintiff's data. Plaintiffs' FAC includes no such allegations.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Further, to protect end users' privacy, AWS is contractually prohibited from "access[ing] or us[ing] . . . Content [of customers] except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." Spear Decl., C ¶ 3.2. As a result, AWS does not know whether (much less when) customers like ProctorU upload *biometric* data to their S3 buckets. Nor does AWS know whether (much less when) its customers upload biometric data from *Illinois residents*. And if AWS is not even aware of any such data—and certainly not in control of it—then it follows that AWS cannot publish a policy reflecting how and when any such data will be deleted.

Similarly, AWS cannot comply with Section 15(a)'s deletion requirements. Again, AWS does not know when its customers, like ProctorU, store *biometric* data from *Illinois* residents. Thus, AWS cannot know when BIPA might apply under Plaintiffs' reading of the law. And even if it could, AWS could not determine when BIPA's deletion requirements have been triggered. As a mere back-end service provider, AWS has no way of knowing its customers' "purpose[s]" for collecting end users' data, or when those "purpose[s]" have been "satisfied." 740 ILCS 14/15(a). AWS also has no way of knowing when an end user has "last interact[ed]" with the AWS customer that collected his or her data, because AWS has no relationship with end users. And, of course, if AWS were to delete end users' data contrary to its customers' wishes, then AWS could incur liability to its customers under the parties' contracts and other authorities.[5]

This case vividly illustrates the practical problems with Plaintiffs' position, which cannot be overstated. To comply with Plaintiffs' reading of Section 15(a), AWS first would have to determine the residency of countless ProctorU end users, as well as the types of data that ProctorU collected from those end users. But that is not all. AWS also would have to do that for *all* of the "[m]illions of [other] customers [that] use AWS every day"—not just ProctorU—as well as all of those customers' many millions of end users. FAC ¶ 2. That simply is not possible.

[5] For these and other reasons, AWS contractually requires customers who use Rekognition to "notify[] [AWS] in the event that any [customer content] stored by [Rekognition] must be deleted under applicable law." Spear Decl., Ex. D (AWS Service Terms) ¶ 50.4.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

Plaintiffs' novel reading of BIPA also would lead to untenable results for large swaths of the economy—not just companies like AWS. For example: Under Plaintiffs' reading, companies that provide cloud-based email services (such as Gmail or Hotmail) would be deemed to be "in possession" of any and all data attached to their users' email messages or stored in their users' accounts. Thus, to comply with BIPA, those providers would have to scan users' messages for biometric data; identify the people from whom that data was collected, or at least identify their state of residency; and then delete emails subject to BIPA, notwithstanding the wishes of the senders and recipients. That is an impossible burden that BIPA's authors never intended. And equally important, imposing that burden on email providers and other cloud providers would thoroughly undermine the privacy interests of consumers—the very interests Plaintiffs purport to champion—by forcing back-end service providers like AWS to scan, analyze, and even destroy consumers' private data and communications.

For all these reasons, Plaintiffs' Section 15(a) claim collapses into incoherence.

2. Plaintiffs allege no facts showing that AWS "collected" their data.

Plaintiffs' Section 15(b) claim fails for similar reasons. Section 15(b) applies only to private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. 740 ILCS 14/15(b). (For brevity, AWS uses the word "collect" to encompass all the operative terms.) But Plaintiffs do not, and cannot, allege that AWS collected their biometric data within the meaning of Section 15(b).

BIPA does not define Section 15(b)'s operative terms. But the structure of the statute helps reveal their meaning. Because the General Assembly included the term "possession" in Section 15(a) but not in Section 15(b), it follows that mere "possession of biometric data is insufficient to trigger Section 15(b)'s requirements." *Heard*, 440 F. Supp. 3d at 965 (collecting cases). Further, the General Assembly must have meant to distinguish "between possessing and collecting biometric information." *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 285–86 (N.D. Ill. 2019). Thus, courts have held that collection requires "something more" than mere

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

possession. *Jacobs*, 2021 WL 3172967 at *2. And that "something more" is an "affirmative act" or "an active step to collect, capture, purchase, or otherwise obtain biometric data." *Id.*; *see also Heard*, 440 F. Supp. 3d at 966 (same).

Plaintiffs do not allege that AWS took any "active step[s]" to collect their data. Indeed, Plaintiffs do not even allege that AWS was aware that ProctorU collected their data. And Plaintiffs certainly do not allege that AWS played any role, active or otherwise, in ProctorU's decision to do so. To the contrary, Plaintiffs allege that AWS was nothing more than a passive service provider, while ProctorU determined what data to collect, when to collect it, and what to do with it. *See, e.g.*, FAC ¶ 35 ("ProctorU requires students to show their faces and their photo IDs on camera to help verify their identities"); *see also, e.g.*, *id.* ¶ 30 (customers like ProctorU "run a command within the Amazon API . . . on the images [they] wish[] to compare"); *id.* ¶¶ 40, 47 (ProctorU "required [Plaintiffs] to submit [their] image[s] as well as an image of a valid identification document"). And, once more, it is worth noting that Plaintiffs' allegations are entirely consistent with AWS's Customer Agreement, which states that AWS customers like ProctorU "are solely responsible for the development, content, operation, maintenance, and use of [their] Content." Spear Decl., C ¶ 4.2.

Other courts have dismissed Section 15(b) claims where, as here, a plaintiff alleges only that a defendant acted as a third-party technology or service provider, not the active collector of end users' data. *See, e.g.*, *Jacobs*, 2021 WL 3172967 at *3 (dismissing Section 15(b) claim where the defendant was not the "active collector" but rather "merely provided the cameras" that another entity allegedly used to collect biometric data); *Namuwonge*, 418 F. Supp. 3d at 286 (similar); *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *1–2 (Ill. Cir. Ct. Aug. 23, 2019) (similar). This Court should reach the same result.[6]

[6] One court has seemed to hold that Section 15(b) may apply to third-party service providers that merely store biometric data. *See Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 779 (N.D. Ill. 2020). AWS respectfully submits that *Figueroa* was wrongly decided, including because it fails to explain how passive storage, without more, amounts to active collection.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

In response, Plaintiffs will likely rely on *Vance v. Amazon.com Inc.*, in which Judge Robart held that plaintiffs adequately alleged active collection by Amazon. *See* 525 F. Supp. 3d 1301, 1313–14 (W.D. Wash. 2021). But the allegations in this case could not be more different. In *Vance*, Amazon allegedly "applied for and downloaded [a] dataset" containing facial images so that it could extract biometric data from those images and use the biometric data "to improve" Amazon's products. *Id.* at 1306. Those allegations sufficed, Judge Robart reasoned, because they suggested that Amazon did more than 'passive[ly] 'possess[]'" plaintiff's biometric data; rather, the allegations suggested that Amazon purposely and deliberately "appl[ied] for and download[ed] the data set" and "us[ed] the biometric data" for its own purposes. *Id.* at 1312–13. Here, Plaintiffs allege no such active or intentional efforts to obtain their data. Nor could they.

Like their Section 15(a) claim, Plaintiffs' Section 15(b) claim not only depends on a misreading of BIPA's language, but also leads to "absurd, inconvenient, [and] unjust consequences" that BIPA's authors never intended. *Solon*, 236 Ill. 2d at 441. Section 15(b) provides that a private entity may not collect biometric data unless it first "(1) informs the subject or the subject's legally authorized representative in writing that [biometric data] is being collected or stored; . . . (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which [biometric data] is being collected, stored, and used; and . . . (3) receives a written release executed by the subject . . . or the subject's legally authorized representative." 740 ILCS 14/15(b). Plaintiffs do not explain how AWS and similarly situated cloud-service providers could comply with those detailed notice-and-consent requirements with respect to data they store on behalf of their customers. And for good reason: they simply could not do so.

Here, for example, Plaintiffs allege that AWS does not interact directly with ProctorU's end users or any of its customers' end users. *See, e.g.*, FAC ¶¶ 5, 42, 49. In addition, AWS is contractually prohibited from "access[ing] or us[ing] . . . Content [of AWS customers] except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

a binding order of a governmental body." Spear Decl., Ex. C (AWS Customer Agreement) ¶ 3.2. It follows that AWS does not know and cannot know when its customers are collecting *biometric* data, let alone when they are collecting biometric data from *Illinois residents*. How, then, could AWS determine when to provide notice to, and obtain consent from, ProctorU's end users—or any of its customers' end users? Further, given that AWS's customers alone determine why they collect data and how long they retain it, how could AWS inform its customers' end users—*in advance*—of "the specific purpose and length of time" for which their data will be collected? And, putting all that aside, through what mechanism could AWS provide notice to and obtain consent from its customers' end users, given that AWS does not interact with those end users and is a mere "behind-the-scenes service for [other] businesses"? FAC ¶ 5. Plaintiffs do not say. Nor do they acknowledge that the logical implication of their position is that every company that operates via the cloud, including but not limited to email providers, would be subject to BIPA's stringent requirements. And those same companies would, in turn, be forced to adopt extremely intrusive measures to comply with BIPA's requirements—even if they never actively collected biometric data from a single Illinois resident or engaged in any conduct in Illinois.

In *Zellmer v. Facebook, Inc.*, the Northern District of California considered a similarly flawed interpretation of BIPA. There, the plaintiff sought to hold Facebook liable under Section 15(b) for allegedly failing to provide notice to, and obtain consent from, "non-users"—i.e., Illinois residents who appeared in photographs uploaded to Facebook by Facebook users, but who were not themselves Facebook users and did not have any relationship with Facebook. The *Zellmer* court rejected the claim, reasoning that it would be "patently unreasonable to construe BIPA to mean that" companies are "required to provide notice to, and obtain consent from," end users "who [are] for all practical purposes total strangers" to the companies. No. 18-cv-01880, 2022 WL 976981, at *3 (N.D. Cal. Mar. 31, 2022). Instead, the court reasoned, the "Illinois legislature clearly contemplated that BIPA would apply [only] in situations where a business had at least some measure of knowing contact with and awareness of the people subject to biometric

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

data collection." *Id*. at *4. Any other interpretation "would lead to obvious and insoluble problems," *id*.; "put [companies] in an impossible situation"; and "impose extraordinary burdens on businesses," contrary to "the Illinois legislature's intent," *id*. at *5.

The same reasoning applies here. According to Plaintiffs, AWS has "[m]illions of customers," "[t]housands" of whom use Rekognition. FAC ¶¶ 2, 4. It is simply not possible for AWS to identify, notify, and obtain consent from millions of end users of AWS customers. Even if it was possible in theory, it would impose mind-boggling burdens on AWS in practice, contrary to the General Assembly's intent. *See Zellmer*, 2022 WL 976981, at *5 (according to the Illinois Supreme Court, "BIPA should not impose extraordinary burdens on businesses"). Fortunately, nothing in BIPA purports to impose such impossible demands. Section 15(b) applies only "where a business ha[s] at least some measure of knowing contact with and awareness of the people subject to biometric data collection." *Id*. at *4. This is not one of those cases.

B. Plaintiffs' Claims Should Be Dismissed Under the Illinois Extraterritoriality Doctrine

Plaintiffs' claims fail for the further reason that Plaintiffs have not alleged, and could not allege, that AWS's purported misconduct occurred primarily and substantially in Illinois. "BIPA does not contain an express provision stating it is intended to apply extraterritorially," i.e., beyond the borders of Illinois. *McGoveran v. Amazon Web Servs., Inc.*, No. 20-cv-1399, 2021 WL 4502089, at *3 (D. Del. Sept. 30, 2021). Thus, BIPA applies only if the defendant's alleged conduct "occurred primarily and substantially in Illinois." *Avery*, 216 Ill. 2d at 187.

Here, Plaintiffs do not, and cannot, plead facts showing that AWS engaged in *any* conduct in Illinois, let alone that AWS's conduct occurred "primarily and substantially" in Illinois. *Id*. Instead, Plaintiffs merely allege that (1) they attended school in Illinois; (2) their Colleges "requir[ed]" them to use "ProctorU's software"; (3) they disclosed images of themselves to ProctorU via ProctorU's service; and (4) ProctorU then "used Amazon Rekognition to perform facial recognition" on those images. FAC ¶¶ 38–51. But neither AWS

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

nor ProctorU are Illinois-based companies. *See id*. ¶ 10 (AWS is "a Delaware corporation with its headquarters in Seattle, Washington"); *see also* Spear Decl., Ex. F (Alabama Secretary of State record indicating that ProctorU is a Delaware corporation with its headquarters in Birmingham, Alabama).[7] Further, Plaintiffs do not allege that ProctorU's S3 buckets are located in Illinois (they are not); that ProctorU used Rekognition in Illinois (it did not); or that Plaintiffs interacted with AWS in Illinois (they did not). *See id.* ¶¶ 42–43, 49–50. Thus, Plaintiffs' allegations do not suggest that AWS engaged in *any* Illinois conduct whatsoever.

This case is much like *McGoveran*, where the District of Delaware dismissed strikingly similar BIPA claims against AWS under the extraterritoriality doctrine. In *McGoveran*, the plaintiffs were Illinois residents who contacted the telephone call centers of John Hancock, a financial services company. *See McGoveran*, 2021 WL 4502089, at *2. Plaintiffs alleged that, when they called John Hancock, their voices were recorded and analyzed by Pindrop Security, a Georgia company acting on John Hancock's behalf. *See id*. Plaintiffs further alleged that Pindrop analyzed those recordings to generate "voiceprints," which plaintiffs characterized as biometric data governed by BIPA. *Id*. And, according to plaintiffs, Pindrop then stored the voiceprints on AWS's servers. *See id*. Based on those allegations, plaintiffs sued AWS and Pindrop under BIPA. AWS moved to dismiss plaintiffs' claims, arguing that the "complaint allege[d] an improperly extraterritorial application of BIPA." *Id*. at *1. The court agreed and dismissed plaintiffs' claims, reasoning as follows:

- First, the court noted that plaintiffs did not allege that their "voiceprints" were "created, possessed, or stored . . . in Illinois." *Id*. at *4.
- Second, "AWS emphasize[d] that its data centers [were] located wholly outside Illinois . . . and Plaintiffs [did] not allege otherwise." *Id*.

[7] The Court may take judicial notice of the fact that ProctorU is incorporated in Delaware and based in Alabama because "courts routinely take judicial notice of a company's certificate of incorporation on a motion to dismiss." *In re Coinstar Inc. S'holder Derivative Litig.*, No. C11-133 MJP, 2011 WL 5553778, at *2 (W.D. Wash. Nov. 14, 2011) (citations omitted).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

- Third, the court rejected the argument that AWS's purported failure to provide BIPA-compliant notice and obtain BIPA-compliant consent occurred in Illinois, both because it "really makes no sense to assign a location for an act that did not occur," and because, "[m]ore fundamentally, that argument depends on the assumption that [AWS was] required to" comply with BIPA in Illinois, but plaintiffs did not allege "any activity in Illinois that would impose such obligations on [AWS]." *Id.*

- Fourth, "[a]t bottom," the only alleged connection between the case and Illinois was plaintiffs' residency in Illinois. But a "plaintiff's residency is not enough to establish an Illinois connection in order to survive a motion to dismiss based on extraterritoriality." *Id*. (citing cases).

In sum, the *McGoveran* court concluded that "John Hancock's activities . . . might be ascribed to Illinois." *Id.* at *6. But "the same [could not] be said for Pindrop and AWS, who were merely third-party contractors performing work for John Hancock," so plaintiffs' claims failed. *Id*.[8]

Here, as in *McGoveran*, Plaintiffs seek to hold AWS liable in its capacity as a back-end service provider to another company (Alabama-based ProctorU), even though AWS has no direct relationship with Plaintiffs and even though AWS has never interacted with Plaintiffs in Illinois or elsewhere. Moreover, as in *McGoveran*, Plaintiffs do not, and cannot, allege that the biometric data supposedly at issue—i.e., alleged scans of Plaintiffs' face geometry—was "created, possessed, or stored . . . in Illinois." *Id*. at *4. And finally, as in *McGoveran*, Plaintiffs rely entirely on the mere fact of their Illinois residency to argue that AWS should be held liable under BIPA. *See, e.g.*, FAC ¶¶ 8–9, 38–51. But as the *McGoveran* court made clear, "[a] plaintiff's residency is not enough to establish an Illinois connection in order to survive a motion to dismiss based on extraterritoriality." *McGoveran*, 2021 WL 4502089, at *4.

Judge Robart's recent order granting summary judgment to Microsoft in *Vance v. Microsoft Corporation* further supports dismissal here. *See* No. C20-1082-JLR, 2022 WL 9983979 (W.D. Wash. Oct. 17, 2022). In *Vance*, plaintiffs sued Microsoft under BIPA, alleging that Microsoft improperly obtained and used their biometric data. But, as Judge Robart pointed

[8] Later, the *McGoveran* court allowed plaintiffs' claims to proceed after they amended their complaint to add specific allegations suggesting that AWS's conduct "occurred principally and substantially" in Illinois. *Id*. (Dkt. 46). Plaintiffs' FAC includes no such allegations.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

out, there was virtually no connection between plaintiff's claims and Illinois other than the plaintiffs' residency. Judge Robart properly held that was insufficient and, relying heavily on *McGoveran*, granted summary judgment to Microsoft. *See id*. at *7–8. This case is effectively identical. Plaintiffs do not allege that AWS engaged in any relevant conduct in Illinois, nor could they. Thus, their claims necessarily fail under the extraterritoriality doctrine.[9]

C. BIPA's Financial-Institution Exemption Bars Plaintiffs' Claims

Putting aside the other fatal flaws described above, Plaintiffs' claims should be dismissed because they violate the plain language of Section 25(c) of BIPA.

1. BIPA may not be applied to "financial institutions," which includes colleges and universities that administer financial aid.

Financial institutions "are already subject to a comprehensive privacy protection regime under" the federal Gramm-Leach-Bliley Act ("GLBA") and its regulations. *Bryant v. Compass Grp. USA, Inc*., 503 F. Supp. 3d 597, 601 (N.D. Ill. 2020). Accordingly, to avoid subjecting those institutions to redundant and contradictory requirements, BIPA's authors exempted them from BIPA's scope entirely. In particular, Section 25(c) of BIPA provides that the law does not apply "in any manner to a financial institution or an affiliate of a financial institution that is subject to [the GLBA] and the rules promulgated thereunder." 740 ILCS 14/25(c).

"Financial institution" is a term of art defined by the GLBA and its regulatory scheme. The term "financial institution" includes "any institution" that is "engaging in financial activities." *See* 15 U.S.C. § 6809(3)(A). The term "financial activities" encompasses things like "[l]ending" money, "transferring" money, and "[p]roviding financial, investment, or economic advisory services." 12 U.S.C. § 1843(k). Both the Consumer Financial Protection Bureau and the Federal Trade Commission have acknowledged that institutions of higher education, like Plaintiffs' Colleges, may qualify as "financial institutions" governed by the GLBA. *See, e.g.*,

[9] On the same day, Judge Robart granted summary judgment to Amazon in a very similar case brought by the same plaintiffs against Amazon. *See Vance v. Amazon.com, Inc.*, No. C20-01084-JLR, Sealed Order (W.D. Wash. Oct. 17, 2022) (Dkt. 135); *see also id*., Dkt. 136 (judgment). AWS will provide a copy of that order when it becomes available.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

12 C.F.R. § 1016.1(b)(2)(ii); Fed. Trade Comm'n, Privacy of Consumer Financial Information, 65 Fed. Reg. 33646, 33648 (May 24, 2000) (explaining that "institutions of higher education" are financial institutions because "[m]any, if not all, such institutions appear to be significantly engaged in lending funds to consumers").

Accordingly, courts have held that Section 25(c) prohibits applying BIPA's requirements to the activities of colleges and universities, *including in the remote proctoring context*. For example, in *Doe v. Northwestern University*, the plaintiff alleged that she was a student at Northwestern University; that Northwestern required her to use "third-party online remote proctoring tools"; and that those third-party services collected and stored her biometric data in violation of BIPA. 546 F. Supp. 3d 841, 841–42 (N.D. Ill. 2022). The court dismissed plaintiff's claims, holding that Northwestern was a financial institution and therefore "exempt from BIPA." *Id*. at 843–44. Even more recently, a different court dismissed similar BIPA claims against Bradley University for the same reasons. *See Duerr v. Bradley Univ.*, No. 21-CV-01096, 2022 WL 1487747, at *7 (C.D. Ill. Mar. 10, 2022).

2. Allowing Plaintiffs' claims to proceed would impermissibly apply BIPA's requirements to the Colleges, which are financial institutions.

Here, BIPA's financial-institution exemption requires dismissal of Plaintiffs' claims.

First, just like Northwestern University and Bradley University, Plaintiffs' Colleges are financial institutions. Like many other institutions of higher learning, the Colleges administer financial aid for their students, and they have been identified by the Federal Student Aid office of the U.S. Department of Education as participants in the Title IV federal student aid program. *See* Spear Decl., Ex. G (listing schools that participate in the Title IV federal student aid program, including the Colleges); Exs. H, I (reflecting the volume of loans originated by participating schools, including the Colleges); *see also Northwestern Univ.*, 586 F. Supp. 3d at 843 (relying on "publicly available government documents" to establish that university offered financial aid). Thus, the Colleges are exempt from BIPA's requirements under Section 25(c).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

In response, Plaintiffs will likely rely on *Patterson v. Respondus, Inc.*, Nos. 20 C 7692, 21 C 1785, 21 C 2620, 2022 WL 860946, at *21 (N.D. Ill. Mar. 23, 2022), which rejected an argument based on Section 25(c). In *Patterson*, the court declined to apply the financial-institution exemption because it was "unwilling to untangle [the] web of agency authority" regarding the GLBA "without the benefit of further briefing." *Id*. at *22. In particular, the *Patterson* court expressed uncertainty about the scope of the FTC's authority to categorize institutions of "higher education" as "financial institutions." *Id*. at *20. But although the court noted that the Consumer Financial Protection Bureau does have broad rulemaking authority under the GLBA, *id*. at *21 (citation omitted), it failed to consider that the CFPB, like the FTC, had already determined that institutions of higher education may qualify as financial institutions. *See* 12 C.F.R. § 1016.1(b)(2)(ii). More importantly, the *Patterson* court did not meaningfully address the fact that colleges are engaged in "[l]ending" money to students—a fact that resolves the "financial institution" inquiry based on the text of the GLBA itself, without regard to any regulator's statements or authority. *See* 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k). Accordingly, AWS respectfully submits that the *Patterson* court's ruling based on "confusion over the breadth of FTC authority" was misguided. *Patterson*, 2022 WL 860946, at *21–22.

Second, the practical effect of applying BIPA to AWS in this context would be to apply BIPA to the Colleges, which is precisely what Section 25(c) forbids.

Plaintiffs acknowledge, as they must, that the remote proctoring activities giving rise to their claims are *the Colleges'* activities. *See* FAC ¶¶ 39, 46 (alleging that the Colleges "requir[ed]" Plaintiffs to use "ProctorU's software"). It follows that Section 25(c) prohibits applying BIPA to those activities. *See Northwestern Univ.*, 586 F. Supp. 3d at 843–44 (dismissing BIPA claims against university based on university's remote proctoring program); *Duerr*, 2022 WL 1487747 at *7 (same). Plaintiffs, however, contend that AWS must provide BIPA-compliant notices to the Colleges' students whenever they use ProctorU's software. *See* FAC ¶¶ 76–77. They also contend that AWS must obtain BIPA-compliant "written releases"

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

from the Colleges' students. *Id.* ¶ 75. And, it appears, Plaintiffs also believe that AWS must delete students' data according to BIPA's requirements, notwithstanding the wishes of ProctorU and the Colleges. Of course, forcing AWS to inject itself into the Colleges' remote proctoring activities in those ways would necessarily interfere with the Colleges' activities, including by forcing the Colleges and ProctorU to redesign the interfaces through which "students sign in to ProctorU to take a test." *Id.* ¶ 36. Indeed, practically speaking, Plaintiffs' BIPA claims would subject the Colleges' remote proctoring activities to all of BIPA's requirements, just from the "bottom up" rather than from the "top down." Section 25(c) does not allow that result.

In response, Plaintiffs may argue that they are not seeking to hold the Colleges liable. They may also argue that requiring the Colleges to modify their remote proctoring programs would impose a minor burden on the Colleges. But Section 25(c) prohibits applying BIPA to the Colleges "in *any* manner." 740 ILCS 14/25(c) (emphasis added). Thus, it requires the Court to reject any reading of BIPA that would impose BIPA's requirements on the Colleges' activities—even indirectly or to a limited extent. *Cf. Stevenson v. FedEx Ground Package Sys., Inc.*, 69 F. Supp. 3d 792, 796 (N.D. Ill. 2014) (Illinois law prohibited interfering with employees' rights "in any manner whatsoever"; court interpreted that language to prohibit even "minor" and "de minimis" interference). Any other reading would require the Court to ignore Section 25(c)'s "in any manner" language, violating basic canons of statutory construction. *See Chestnut Corp. v. Pestine, Brinati, Gamer, Ltd.*, 667 N.E.2d 543, 547 (Ill. App. Ct. 1996) ("Statutes are to be construed to give full effect to each word, clause, and sentence, so that no word, clause, or sentence is surplusage or void.") (citation omitted).

D. Plaintiffs Cannot Be "Aggrieved" by AWS's Alleged Violation of Section 15(a)

Plaintiffs' Section 15(a) claims fail for an additional and independent reason: Plaintiffs cannot show that they are "aggrieved" by AWS's alleged violation of Section 15(a), which is a threshold requirement for bringing a claim under BIPA.

Only an "aggrieved" person may seek relief under BIPA. 740 ILCS 14/20. And to be

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

aggrieved, a plaintiff must "hav[e] legal rights that are adversely affected" or "invaded" by the defendant's conduct. *Rosenbach*, 129 N.E.3d at 1205. Thus, to show that they are aggrieved for purposes of their Section 15(a) claim, Plaintiffs must plausibly allege both that (1) AWS violated a legal duty under Section 15(a), and (2) that AWS owed that legal duty to Plaintiffs. *See, e.g.*, *Am. Sur. Co. v. Jones*, 51 N.E.2d 122, 125 (Ill. 1943) (appellants were not "aggrieved" because the action of which they complained "did not directly affect [their] interest"); *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. 535, 546 (N.D. Cal. 2018) (holding that "a party is aggrieved" under BIPA "by an act that directly or immediately affects her legal interest").

Plaintiffs cannot meet those requirements. They allege that AWS violated Section 15(a) by "fail[ing] to publicly provide a retention schedule or guideline for permanently destroying" biometric data. FAC ¶ 66. But "the duty to disclose under section 15(a) is owed to the public generally, *not to particular persons*." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020) (emphasis added). Plaintiffs have therefore alleged, at most, that AWS violated a duty owed to *the public*, not to *them individually*. Thus, they are not "aggrieved," and their claim necessarily fails.

E. AWS Complied with BIPA

Finally, even if Plaintiffs could overcome all the obstacles above and show that BIPA applies to AWS in this context, it would not matter. Because AWS complied with BIPA, Plaintiffs' claims necessarily fail on their own terms.

No statute requires the impossible. *See Midwest Bank & Tr. Co. v. Roderick*, 476 N.E.2d 1326, 1331–32 (Ill. App. 1985) (statutory interpretation is "unfair and unreasonable" if it would impose a requirement that "could very well be impossible to meet"). BIPA is no different. *See, e.g.*, *Rosenbach*, 129 N.E.3d at 1207 (explaining that BIPA "[c]ompliance should not be difficult"). Thus, courts have held that back-end service providers that do not interact with their customers' end users—i.e., service providers like AWS—may comply with BIPA by contractually requiring their customers to comply with BIPA. *See Figueroa*, 454 F. Supp. 3d at

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000

783 (explaining that a service provider "could have complied" with BIPA by requiring its customers "as a contractual precondition of using [the service provider's] biometric timekeeping device, to agree to obtain their employees' written consent to [the service provider] obtaining their data"); *see also Ronquillo v. Doctor's Assocs., LLC*, No. 21 C 4903, 2022 WL 1016600, at *3 (N.D. Ill. Apr. 4, 2022) (same) (citation omitted). And, to their credit, Plaintiffs themselves seem to acknowledge that service providers like AWS may comply with BIPA by contractually requiring their customers to comply. *See* FAC ¶¶ 42, 49 ("At no time did Plaintiff[s] . . . receive notice from AWS, *whether through ProctorU or otherwise*, that AWS was collecting, storing, and using [their] biometric data.") (emphasis added).

That is exactly what AWS did. Under AWS's Service Terms, all AWS customers who use Rekognition (including ProctorU) are contractually required to "provid[e] legally adequate privacy notices to End Users" (including Plaintiffs). Spear Decl., Ex. D (AWS Service Terms) ¶ 50.4. Similarly, all such AWS customers are required to "obtain[] necessary consent from such End Users." *Id*. AWS customers are also obligated to ensure compliance with other BIPA requirements, including BIPA's retention and deletion requirements. *Id*. Plaintiffs have not alleged that AWS could have or should have done anything more, or anything different, to comply with BIPA. Nor could they. Their claims fail for that reason, as well.

CONCLUSION

AWS respectfully requests that the Court dismiss Plaintiffs' claims with prejudice.

Dated: October 19, 2022

By: */s/ Ryan Spear*

Ryan Spear, WSBA No. 39974
RSpear@perkinscoie.com
Nicola Menaldo, WSBA No. 44459
NMenaldo@perkinscoie.com
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone 206.359.8000
Facsimile 206.359.9000
Attorneys for Defendant Amazon Web Services, Inc.